UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF VERMONT

UNITED STATES OF AMERICA, v. BRIAN FOLKS, Defendant.	Crim. No. 5:16-CR-94-1

GOVERNMENT'S OPPOSITION TO DEFENDANT'S MOTION TO SUPPRESS EVIDENCE

The United States of America, by and through its attorney, Christina E. Nolan, United States Attorney for the District of Vermont, files this response to defendant Brian Folks' Motion to Suppress Evidence Re: Search Warrant for Five Communication Devices (Doc. 144) ("the Motion") obtained from four electronic storage media devices (collectively, the "electronic devices" or "devices")[1] that were lawfully seized on July 19, 2016, and subsequently searched in accordance with a Federal Rule of Criminal Procedure 41 search warrant issued by the Honorable John M. Conroy on January 27, 2017 ("the search warrant").

I. INTRODUCTION

In the instant Motion, the defendant neither challenges the initial seizure of the devices[2] nor denies that the search warrant affidavit established probable cause to search the devices for records relating to, or constituting evidence of, violations of 21 U.S.C. §§ 841(a) and 846, and 18

[1] Despite the Motion's title, the defendant only moves to suppress evidence obtained from two cell phones seized from the defendant at the time of arrest on July 19, 2016, and a tablet and computer that were seized during the execution of a search warrant for the premised located at 96 Ethan Allen Parkway, Unit #8, Burlington, Vermont on July 19, 2016. *See* Mot. at 1-2. Thus, this response will only address those issues raised in Docket No. 144.

[2] Footnote 2 of the Motion clarifies that it raised its objections to the initial seizure of the devices in a separate motion to suppress. *See* Mot. 2 n.2 (citing Doc. 143).

U.S.C. §§ 1591 and 922(g)(l). Instead, the Motion objects only to the timeliness and manner of the government's compliance with Rule 41's two-step approach to warrants to search electronic devices, as well as arguing that the search warrant should have imposed additional, unspecified minimization procedures.

As explained below, the defendant's Motion fails because the government properly followed Rule 41(e)(2)(b)'s two-step approach to search warrants for electronic evidence: the government initiated the process to forensically image the electronic media identified in Attachment A of the warrant within 14 days of the warrant's issuance, *see* Rule 41(e)(2)(A) and (f)(1)(A), and thereafter diligently performed an off-site review of the imaged media to seize the information set forth in Attachment B of the warrant. The government's imaging, review, and retention of information was appropriate and constitutionally reasonable under relevant Fourth Amendment precedent. In addition, Attachment B of the search warrant appropriately cabined the government's search of the electronic devices by identifying the target (*i.e.*, the defendant) and criminal conduct under investigation, as well as specifying particular categories of information to be seized. No further minimization procedures were required under the Fourth Amendment. Further, if a Constitutional violation had occurred (it did not), the defendant's request for a suppression remedy fails because it was objectively reasonable for the executing officers to rely on the search warrant.

II. BACKGROUND

Defendant Brian Folks is charged in the Fourth Superseding Indictment with conspiracy to distribute heroin and cocaine base, being a felon in possession of a firearm, five substantive counts of distribution of and possession with intent to distribute narcotics, six counts of human

trafficking, and interstate travel in aid of racketeering ("ITAR"). The Fourth Superseding Indictment concerns an approximately four-year period from June 2012 to March 2016, inclusive. On July 14, 2016, based on a twenty-two page affidavit by Drug Enforcement Administration ("DEA") Special Agent Adam Chetwynd, Magistrate Judge John M. Conroy issued a search warrant for 96 Ethan Allen Parkway, Unit #8, Burlington, Vermont, the residence of Danielle Degenhardt. On July 19, 2016, two items covered in the Five Communication Devices Search Warrant were seized pursuant to the search warrant at 96 Ethan Allen Parkway: a Black Trio Stealth 10 tablet computer S/N: 1401474269 (DEVICE FOUR) and an HP Pavilion Series Computer Tower S/N: MXU13503T4 (DEVICE FIVE).

Also on July 19, 2016, two items covered in the Five Communication Devices Search Warrant were seized incident to arrest: At the time of FOLKS' arrest, two cellular devices were in his possession (DEVICES ONE AND TWO).[3]

On January 27, 2017, based on a twenty-four page affidavit by Drug Enforcement Administration ("DEA") Task Force Officer Robert Estes, Magistrate Judge John M. Conroy issued a search warrant for the contents of and records relating to five electronic devices: Search Warrant for Five Communication Devices. The affidavit and its Attachment B specified that there was probable cause to believe that the electronic devices contained fruits, evidence and instrumentalities of violations of (i) distribution of controlled substances and conspiracy to distribute controlled substances in violation of 21 U.S.C. §§ 841(a) and 846; (ii) sex trafficking, in violation of 18 U.S.C. § 1591; and (iii) the illegal possession of a firearm by a convicted felon in violation of 18 U.S.C. § 922(g)(1).

[3] When uncharged co-conspirator Victor GIBSON was arrested, the fifth item, a cellular device, was in his possession (DEVICE THREE). The search of this device is not challenged in the instant motion.

On the very same day that it secured the search warrant, DEA properly initiated the process to forensically image the electronic media identified in Attachment A of the warrant as required by Rule 41(e)(2)(A) and (f)(1)(A) (requiring initiation of this process within 14 days of the warrant's issuance). Following the swearing of the search warrant at 11:15 am, that afternoon DEA immediately opened the devices that they could access and realized that they needed assistance as DEA Burlington does not have the forensic resources necessary to access at least one of the devices seized (namely, the HP computer hard drive), due to multiple user profiles and associated passwords. After securing the permission of the Office for the United States Attorney for the District of Vermont to enlist the help of a forensic expert, DEA delivered all of the devices to the expert on February 3, 2017. Frank Thornton began his forensic imaging work on February 3, 2017, also within the fourteen-day window (which expired on February 10, 2017). On April 24, 2017, Thornton provided DEA with a one-terabyte size hard drive loaded with all of the forensic extractions and the reports associated with each device. Thereafter, DEA commenced a review of the imaged data for responsiveness under Attachment B. A copy of this responsive data was turned over and/or made available to the defense for review on May 31 and June 7, 2017. DEA securely retains both a mirror image copy of the raw, extracted data and a copy of the segregated, responsive data.

Attachment A properly identified the items to be searched as follows:

1. The property to be searched is the content of five communication devices as follows:

    a. Silver Samsung Galaxy S6 smartphone (IMEI: 359652062439497, S/N: R38GA0Q5DJA), hereafter referred to as DEVICE ONE;

    b. Black Microsoft smartphone (Model: RM-1073, IMEI: 357816060778576), hereafter referred to as DEVICE TWO;

c. Silver LG smartphone (Model : LGMS330, IMEI: 359696071233953, S/N: 604CYMR123395), hereafter referred to as DEVICE THREE;

d. Black Trio Stealth 10 tablet (S/N: 1401474269), hereafter referred to as DEVICE FOUR;

e. Black Hewlett-Packard Pavilion computer (S/N: MXU13503T4), hereafter referred to as DEVICE FIVE;

2. DEVICE ONE, DEVICE TWO and DEVICE THREE are currently in the possession of DEA. DEVICE FOUR and DEVICE FIVE are in the possession of the Federal Bureau of Investigation (FBI). DEA transferred possession of these two devices to the FBI following seizure.

3. The applied-for warrant would authorize the forensic examination of the five communication devices for the purpose of identifying electronically stored data particularly described in Attachment B.

Attachment B identified the items to be seized with the following illustrative detail:

1. All records on the five communication devices that relate to, or constitute evidence of, violations of federal laws, including but not limited to the possession with intent to distribute heroin, conspiracy to distribute heroin, sex trafficking, and the unlawful possession of a firearm, in violation of 21 U.S.C. §§ 841(a) and 846; 18 U.S.C. §§ 1591 and 922(g)(1), committed by Brian FOLKS and his known and unknown associates and coconspirators, including:

a. telephone numbers in contact lists including names and phone numbers of coconspirators, customers, and other associates and related identifying information and the telephone number assigned to the phone, records of telephones to which calls were placed and from which calls were received as well as logs of incoming, outgoing, and missed calls;

b. types, amounts, and prices of drugs and persons trafficked as well as dates, places, and amount of specific transactions;

c. any information related to sources of drugs (including names, addresses, phone numbers, or any other identifying information);

d. any information related to the identity of persons trafficked, as well as dates, places, and amount of specific transactions;

e. location information of the phone at various times as provided by the metadata associated with photographs and location information provided by GPS applications;

f. any information regarding bank records, checks, credit card bills, account information, commercial exchanges, and other financial records;

g. text, numeric, and alphanumeric messages;

h. digital photographs and videos of individuals involved in drug or human trafficking, of drug or commercial sex proceeds, controlled substances, cash, hotel rooms, automobiles used to transport controlled substances, and drug- or sex-related paraphernalia.

2. Evidence of user attribution (including the purpose of its use, who used it, and when), showing who used or owned the five communication devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.
3. As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of electronic or computer storage.

III. ARGUMENT

A. The Search Warrant Was Executed According to Rule 41's Two-Step Procedure for Electronic Warrant.

a. The Search Warrant Was Executed In A Timely Fashion

As set forth above, DEA attempted to forensically image the four challenged electronic devices identified in Attachment A of the search warrant on the day (January 27, 2017) the warrant was issued by the Court. Further, after confronting certain obstacles to the extraction of all of the data authorized by the search warrant, the electronic devices were provided to a digital forensic contractor, Frank Thornton, who began the forensic imaging on February 3, 2017, also within the fourteen-day window. As explained below, the government's attempts to initiate the forensic imaging of the devices satisfy the government's obligation to "execute" the warrant prior to the February 10, 2017 deadline established by the search warrant and Rule 41

and comport with step one of Rule 41(e)(2)(B)'s well-established two-step approach to warrants for electronic evidence. The defendant's insistence that the warrant required the Government to complete its forensic review of the electronic devices by February 10, 2017 is contradicted by the plain language of Rule 41(e)(2)(B), established caselaw, and the terms of the search warrant and supporting affidavit.

Rule 41(e)(2)(B) specifies that a warrant seeking electronically stored information "may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information." It then presumes a later, off-site review that extends beyond Rule 41's traditional 14-day window by providing, in relevant part, that "[u]nless otherwise specified, the warrant authorizes ***a later review*** of the media or information ***consistent with the warrant***. The ***time for executing*** the warrant in Rule 41(e)(2)(A) and (f)(1)(A) refers to the seizure or on-site copying of the media or information, and ***not to any later off-site copying or review***." *Id*. (emphasis added). As Rule 41(e)(2)(B) plainly indicates, the phrase "consistent with the warrant" refers to the parameters of the search set forth in the attachments and supporting affidavit application, and does not require that the face of the AO 93 form of the warrant identify a definitive date for the review's completion. To the contrary, Rule 41 is unambiguous that, "unless otherwise specified," the 14-day deadline for executing a warrant refers only to the initial step of seizing or copying the media or information.

Indeed, the Advisory Committee Notes explain that the two-step process is "inherent in searches for electronically stored information." Fed. R. Crim. P. 41, Advisory Committee's Notes (2009 amend.). The Notes recognize that electronic storage media "commonly contain such large amounts of information that it is often impractical for law enforcement to review all of

the information during execution of the warrant at the search location." *Id.* They also note that "[a] substantial amount of time can be involved in the forensic imaging and review of information. This is due to the sheer size of the storage capacity of media, difficulties created by encryption and booby traps, and the workload of the computer labs." *Id*.

In view of these practical considerations, federal courts have routinely found that off-site forensic analyses and reviews that take as long as many months or even years to complete comply with Rule 41's two-step process, and are reasonable under the Fourth Amendment. *See, e.g.*, *United States v. Stabile*, 633 F.3d 219, 233-34 (3d Cir. 2011) ("practical realities of computer investigations preclude on-site searches"); *United States v. Brewer*, 588 F.3d 1165, 1173 (8th Cir. 2009) ("Because of the nature of this evidence, the several months' delay in searching the media did not alter the probable cause analysis."); *United States v. Grimmett*, 439 F.3d 1263, 1268-70 (10th Cir. 2006) (search warrant for "any and all" computer hardware and software for child pornography authorized both seizure and later search of the defendant's computer files); *United States v. Alston*, No. 15-CR-435, 2016 WL 2609521, at *3-4 (S.D.N.Y. Apr. 29, 2016) (finding that the Government complied with Rule 41's time requirements by "attempting to access the phone within the period specified in the warrant" under circumstances where it took three months to ultimately decrypt and access the data); *United States v. Winther*, No. 11-CR-212, 2011 WL 5837083l, at *10-14 (E.D. Pa. Nov. 18, 2011) (rejecting the argument that the "unless otherwise specified" language of Rule 41(e)(2)(B) required the forensic analysis of the computer to be completed within 14 days of the warrant's issuance, and affirming the constitutional reasonableness of the search).

The search warrant at issue here is no different. The AO 93 cover sheet of the warrant

specified only a February 10, 2017 deadline for seizing or copying the electronic devices, and incorporated by reference complimentary Attachments A and B that set forth a two-step approach to their search. The affidavit supporting the search warrant further clarified that, consistent with Rule 41(e)(2)(B), the Government's search would require a forensic review of the electronic devices that "*may take longer than 10 days to complete*." *See* Robert Estes, Search Warrant Affidavit ("Estes Aff.") ¶¶ 34-35 (emphasis added). To explain the need for a fulsome, off-site review, the affidavit detailed how the government would perform a forensic review to obtain forensic evidence relating to, among other things, the editing or deletion of files, user attribution, and contextual data concerning the devices' use. *See id*. ¶ 34. The affidavit also explained that a review of "electronically stored information on a storage medium is a dynamic process" that requires iterative analysis by investigators familiar with the case and the context of evidence, *id*. ¶ 34, and may require the deployment of a variety of forensic techniques, such as "computer-assisted scans of the entire medium, that might expose many parts of the devices to human inspection in order to determine what is seizable evidence described by the warrant. *Id*. ¶ 35.

Accordingly, by initiating the forensic review of the electronic devices before February 10, 2017, the Government fully complied with its obligation under the warrant and Rule 41(e)(2)(B) to "execute" the warrant in accordance with the timing set forth Rule 41(e)(2)(A) and (f)(1)(A). Further, after execution, the forensic examiner extracted the evidence from the electronic devices in a reasonably diligent manner, and he returned the devices, the imaged data, and the reports associated with his work to DEA on April 24, 2017. Thereafter, DEA commenced its review of the imaged data for responsiveness under Attachment B.

b. The Government's Forensic Imaging of the Electronic Devices Complies With Rule 41's Two-Step Procedure For Electronic Evidence, And Is Consistent With the Fourth Amendment

The Defendant's Motion also contends that the government executed the search warrant as a "general warrant" by impermissibly 'seizing' evidence that was not described in Attachment B of the search warrant. *See, e.g.*, Mot. 4-5. However, the defendant fails to identify any specific evidence that (he alleges) was improperly seized. Indeed, although fashioned as an execution-based challenge, *see* Mot. 7, the Defendant appears to facially attack Rule 41's two-step process by wrongly insisting that the government "seized" all of the data stored on the electronic devices when it merely generated forensic images of the devices identified in Attachment A—*i.e.*, the first step of Rule 41's two-step procedure for electronic evidence. *See, e.g., id.* This is simply inaccurate. In accordance with the search warrant and Rule 41's two-step framework, the government only seized records and information authorized by Attachment B of the search warrant. As explained below, the government's creation and retention of forensic copies of the searched media to facilitate the seizure of information authorized in Attachment B complies with Rule 41's two-step process and is a process that federal courts around the country have repeatedly approved, including the Second Circuit. *See, e.g., United States v. Ulbricht*, 858 F.3d 71 (2d Cir. 2017).

As noted above, Rule 41(e)(2)(B)'s two-step approach to search warrants for electronic evidence is a practical necessity given the substantial storage capacity of electronic media, challenges associated with forensically analyzing data, and the workload of computer labs. *See, e.g.*, Fed. R. Crim. P. 41, Advisory Committee's Notes (2009 amend.); Estes Aff. ¶¶ 34-35. Further, as the affidavit supporting the search warrant detailed, a forensic review of electronic evidence is a "dynamic process" that cannot be easily concluded by a review team that is

unfamiliar with the investigation or familiar with the operation of the storage media being searched. *See* Estes Aff. ¶¶ 34-35.

In view of these practical considerations, federal courts have long affirmed the constitutional reasonableness of the government, as it did here, forensically copying electronic media in accordance with Rule 41's two-step approach to warrants for electronic evidence. *See, e.g.*, *Ulbricht*, 858 F.3d at 100-104 ("[A] broad warrant allowing the government to search his laptop for potentially extensive evidence of those crimes does not offend the Fourth Amendment . . . ."); *Stabile*, 633 F.3d at 233-34; *Grimmett*, 439 F.3d at 1268-70; *Guest v. Leis*, 255 F.3d 325, 335 (6th Cir. 2001) ("Because of the technical difficulties of conducting a computer search in a suspect's home, the seizure of the computers, including their content, was reasonable in these cases to allow police to locate the offending files."); *United States v. Hay*, 231 F.3d 630, 637-38 (9th Cir. 2000) (holding that officers were justified in removing computers for off-site search "because of the time, expertise, and controlled environment required for a proper analysis"); *United States v. Upham*, 168 F.3d 532, 535 (1st Cir. 1999) ("As a practical matter, the seizure and subsequent off-premises search of the computer and all available disks was about the narrowest definable search and seizure reasonably likely to obtain the [evidence sought]."). As the Sixth Circuit explained, "[t]he federal courts are in agreement that a warrant authorizing the seizure of a defendant's home computer equipment and digital media for a subsequent off-site electronic search is not unreasonable or overbroad, as long as the probable-cause showing in the warrant application and affidavit demonstrate a 'sufficient chance of finding some needles in the computer haystack.'" *United States v. Evers*, 669 F.3d 645, 652 (6th Cir. 2012).

In addition, contrary to the defendant's claim (*see* Mot. at 4-5), a defendant's Fourth

Amendment rights are not violated when the government incidentally accesses non-relevant material in the course of searching an electronic media for evidence that falls within the scope of the search warrant. *See, e.g.*, 858 F.3d at 103-104. Indeed, as the Second Circuit recently explained in *Ulbricht*, 858 F.3d at 103, the exposure of some personal data of the defendant to cursory review is "inevitable . . . in almost any warranted search because in 'searches for papers, it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized.'" *Id*. at 103 (citing *United States v. Ganias*, 824 F.3d 199, 211 (2d Cir. 2016) (en banc)) (citations omitted). Where, as here, there is no reason to doubt the faithful execution of the warrant,[4] the Fourth Amendment's protections against "unwarranted intrusions upon privacy" are adequately ensured "by requiring a warrant to describe its scope with particularity." *Id*. at 103.

The government's retention of the original electronic devices and their mirror copies was also reasonable under the Fourth Amendment. *First*, after initially determining which electronic information fell within the Warrant's scope, the government did not then attempt to review any electronic evidence deemed outside its scope. The mere retention of data where is it not searched any further is not a search and seizure and therefore not a basis for suppression. *Second*, a number of federal courts have also held that, as here, it is reasonable for the government to preserve, during the pendency of an ongoing investigation, originals and/or mirror copies of the seized electronic evidence to, among other things, "permit the accurate extraction of the primary evidentiary material sought pursuant to the warrant[s]; to secure metadata and other probative evidence stored in the interstices of the storage medium; and to

[4] Beyond speculation, the defendant's Motion offers no evidence to suggest that the government failed to faithfully execute the warrant in accordance with the two-step process authorized by the Court.

preserve, authenticate, and effectively present at trial the evidence thus lawfully obtained." *Ganias*, 824 F.3d at 216 (describing the reasons why it may be necessary to preserve original copies of a storage medium); *see, e.g.*, *United States v. Johnson*, 789 F.3d 934, 941-43 (9th Cir. 2015) (denying suppression motion where defendant complained about a third, more exhaustive search of computer for items within scope of initial warrant that was conducted five years after initial searches); *United States v. Scully*, 108 F. Supp. 3d 59, 100-01 (E.D.N.Y. 2015) (denying motion to suppress emails as outside of scope of warrant because retention for two and a half years was for authentication purposes); *United States v. Kenner*, No. 2:13-cr-00607-JFB, Doc. 329, slip. Op. at 5-7 (E.D.N.Y. 2015) (denying motion to suppress evidence based on government's retention of hardware and imaged copies for approximately 16 months).

The Second Circuit's reasoning in *United States v. Ganias*, 824 F.3d 199 (2d Cir. 2016) ("*Ganias II*")[5] is instructive. The defendant in that case had moved to suppress evidence seized in connection with a 2006 warrant on the grounds that the government violated his Fourth Amendment rights when, after lawfully copying three of his hard drives for off-site review pursuant to a 2003 search warrant, it retained these full forensic copies (or "mirrors"), which included data both responsive and non-responsive to the 2003 warrant, while its investigation continued, and ultimately searched the non-responsive data pursuant to a second warrant three years later, in 2006. *Id.* at 201-03. The en banc court concluded that suppression was an inappropriate remedy because it was "objectively reasonable" for the government to rely in good faith on the search warrant at issue, *id*. at 221-24, and elected not to "decide whether retention of

[5] The Second Circuit's decision in *United States v. Ganias*, 824 F.3d 199 (2d Cir. 2016) ("*Ganias II*") reversed the holding of a divided Second Circuit panel in *United States v. Ganias*, 755 F.3d 125 (2d Cir. 2014) ("*Ganias I*), which had granted the defendant's motion to suppress evidence based on the government's retention of data.

the forensic mirrors violated the Fourth Amendment," *id.* at 200.

However, the *Ganias II* court detailed a number of the unique features of a digital search that may make it reasonable for the government to retain a forensic copy of electronically stored data. For example, the Second Circuit explained that "[e]ven the most conventional 'files'—word documents and spreadsheets such as those the Government searched in this case – are not maintained, like files in a file cabinet, in discrete physical locations separate and distinct from other files," but rather are "fragmented" across physical locations. *Id.* at 213. Moreover, a "computer stores unseen information about any given 'file,'" such as "metadata about when the file was created or who created it" and "prior versions or edits that may still exist . . . –further interspersing the data corresponding to that 'file' across the physical storage medium." *Id.* Files therefore "are not as discrete as they may appear to a user," and "[t]heir interspersion throughout a digital storage medium . . . may affect the degree to which it is feasible . . . to fully extract and segregate responsive data from nonresponsive data." *Id.* Courts therefore "must be attuned to the technological features unique to digital media as a whole and to those relevant in a particular case – features that simply do not exist in the context of paper files." *Id.*

Ganias II did not limit its discussion to computer "files"; the court also noted "that a good deal of the information that a forensic examiner may seek on a digital storage device . . . does not even remotely fit into the typical user's conception of a 'file.'" *Id.* The Court went on to describe such information, including "evidence sufficient to reconstruct a deleted file," "metadata about a user's activities, or the manner in which information has been stored, to show such things as knowledge and intent," and evidence "that something *did not happen*," such as a virus attack. *Id.* at 213-14.

Because of these complexities, the *Ganias II* court recognized the "potential challenges to parties seeking to preserve digital evidence, authenticate it at trial, and establish its integrity for a fact-finder – challenges that materially differ from those in the paper file context." *Id.* at 215. The Court again gave examples, including that extracting "specific data files . . . can alter, omit, or even destroy portions of the information," and that therefore "[p]reservation of the original medium or a complete mirror may be necessary in order to safeguard the integrity of evidence that has been lawfully obtained or to authenticate it at trial." *Id.* Such preservation "is not simply a concern for law enforcement[,]" but "may also be necessary to afford criminal defendants access to that medium or its forensic copy so that, relying on forensic experts of their own, they may challenge the authenticity or reliability of evidence allegedly retrieved. *Id.*

For all of these reasons, the *Ganias II* court, while not deciding the issue, remarked that the government had "plausibly" argued that a digital storage medium or its forensic copy may need to be retained during the course of an investigation and prosecution, to permit the accurate extraction of the primary evidentiary material sought pursuant to the warrant; to secure metadata and other probative evidence stored in the interstices of the storage medium; and to preserve, authenticate, and effectively present at trial the evidence thus lawfully obtained.
Id. at 216.

The reasoning underlying the en banc ruling in *Ganias II* and a number of successor rulings underscores the reasonableness of the government's retention of electronically stored information in this case. *See, e.g.*, *Scully*, 108 F. Supp. 3d at 100-01. For instance, Attachment B of the search warrant expressly authorizes the Government to seize forensic data relevant to user attribution, such as evidence showing "who used or owned the five

communication devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history." Further, as the affidavit supporting the search warrant detailed, the type of forensic review necessitated by this matter demands a "dynamic process" where the relevancy of certain pieces of forensic evidence to items within the scope of the search warrant may only become apparent after information is iteratively learned through investigative steps and analyses. *See, e.g.*, *id.*

Accordingly, for the reasons set forth above, it was reasonable for the Government to retain forensic copies of the electronic devices identified in Attachment A to facilitate the seizure of information authorized in Attachment B.

B. The Search Warrant Need Not Incorporate Minimization Procedures To Comply With the Fourth Amendment

It is a long-recognized canon of Constitutional law that "[t]he Fourth Amendment requires that search warrants be issued only 'upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.'" *Dalia v. United States*, 441 U.S. 238, 255 (1979) (quoting *Stanford v. Texas*, 379 U.S. 476, 481 (1965)). The Supreme Court has interpreted these words to require only three things: issuance by a neutral magistrate, an applicant's demonstration of probable cause to believe that the evidence sought will aid in a particular apprehension or conviction for a particular offense, and particularity in the description of the things to be seized and the place to be searched. *Id.* (internal citations omitted). Critically,

> [n]othing in the language of the Constitution or in th[e Supreme] Court's decisions interpreting that language suggests that, in addition to the three requirements discussed above, search warrants also must include a specification

> of the precise manner in which they are to be executed. On the contrary, ***it is generally left to the discretion of the executing officers to determine the details of how best to proceed with the performance of a search authorized by warrant*** —subject of course to the general Fourth Amendment protection "against unreasonable searches and seizures."

Id. at 257 (emphasis added); *see also U.S. v. Grubbs*, 547 U.S. 90, 98 (2006) (holding that the particularity requirement does not require conditions precedent to execution of an anticipatory warrant). "The general touchstone of reasonableness which governs Fourth Amendment analysis . . . governs the method of execution of the warrant." *United States v. Ramirez*, 523 U.S. 65, 71 (1998) (internal citation omitted).

Despite the Supreme Court's longstanding resistance to prescribing how warrants are executed, the defendant's Motion relies on language from a Ninth Circuit opinion in *United States v. Comprehensive Drug Testing, Inc.*, 579 F.3d 989, 993 (9th Cir. 2009) ("*CDT I*"), as well as stray dicta from other highly distinguishable opinions, to argue wrongly that the search warrant necessarily violated the Fourth Amendment by not including certain unspecified "minimization procedures." *See* Mot. 7-14. As explained below, the defendant misstates the ultimate holding of *CDT I*, inaccurately describes the law in the Second Circuit, and fails to point to a single case that would support his clearly inappropriate request for suppression.

As an initial matter, the defendant is wrong to claim that the *CDT I* protocols for searching digital evidence are mandatory rules that "must" be followed to comply with the Fourth Amendment. *See* Mot. 8. To the contrary, after *CDT I* was issued, the Ninth Circuit itself took the highly unusual step of vacating and superseding *CDT I* with a *per curiam* opinion that omitted the procedural steps that the prior opinion had endorsed. *United States v. Comprehensive Drug Testing, Inc.*, 579 F.3d 989, 993 (9th Cir. 2009), *withdrawn and*

superseded, 621 F.3d 1162 (9th Cir. 2010) (en banc) ("*CDT II*").[6] Accordingly, within even the Ninth Circuit, the *CDT I* prescriptions on data segregation and search protocols are nothing more than "suggestions" for magistrate judges that do not constitute binding Ninth Circuit law. *See CDT II*, 621 F.3d at 1183, Callahan J. (concurring) ("The concurrence is not joined by a majority of the en banc panel and accordingly the suggested guidelines are not Ninth Circuit law."); *see, e.g., United States v. King*, 693 F. Supp. 2d 1200, 1229 (D. Haw. 2010) ("The *CDT* opinion itself does not claim to base its "procedures" on the Fourth Amendment.").

Further, outside of the Ninth Circuit, the majority of courts have declined to follow *CDT I*'s call to impose *ex ante* restrictions that prescribe how the government executes a Rule 41 search warrant for electronic evidence during the course of an ongoing investigation (*e.g.*, until trial). *See, e.g.*, *United States v. Mann*, 592 F.3d 779, 784 (7th Cir. 2010) (criticizing *CDT I* and refusing to impose search protocols); *United States v. Stabile*, 633 F.3d 219, 241 n.16 (3d Cir. 2011) (same); *United States v. Farlow*, 2009 WL 4728690, *6 (D. Me. Dec. 3, 2009). Courts within the Second Circuit have followed the same approach. For instance, in *United States v. Galpin*, 720 F.3d 436, 451 (2d Cir. 2013), the Second Circuit explained that "[u]nlike the Ninth Circuit, we have not required specific search protocols or minimization undertakings as basic predicates for upholding digital search warrants, and we do not impose any rigid requirements in that regard at this juncture."[7] More recently, in *United States v. Alston*, 2016

[6] The defendant's Motion inaccurately characterizes *CDT II* as merely a "revised" opinion.

[7] The defendant's reliance on *United States v. Galpin*, 720 F.3d 436 (2d Cir. 2013) and *United States v. Wey*, 256 F. Supp. 3d 355 (S.D.N.Y. 2017) is misplaced and unavailing. *See* Mot. 10-14. *First*, neither opinion endorses the *ex ante* guidelines set forth in *CDT I* nor suggests, as the defendant does, that the mere absence of minimization procedures constitutes a Fourth Amendment violation. In fact, the Second Circuit ruled precisely the opposite in *Galpin*, 720 F.3d at 451. *Second*, both courts only referenced privacy concerns raised by *CDT* to highlight the importance of digital search warrants complying with the Fourth Amendment's "particularity" requirement. *Galpin*, 720 F.3d at 447 ("This threat demands a heightened sensitivity to the particularity requirement in the context of digital searches."); *Wey*, 256 F. Supp. 3d at 382-83. Here, the *Galpin* and *Wey* concerns about particularly are

WL 2609521 (S.D.N.Y. Apr. 29, 2016), the district court rejected a similar *CDT*-based challenge to a search of electronic evidence that was conducted pursuant to a search warrant that did not include search protocols. *Id.* at *7. In affirming the reasonableness of the search under the Fourth Amendment, the court in *Alston* reiterated that courts within the Southern District of New York have "repeatedly declined to 'impose *ex ante* restrictions pertaining to the later execution of [a] warrant,' and have declined to find searches conducted without such protocols to be impermissible." *Id*. (internal quotations and citations omitted); *see, e.g.*, *United States v. Romain*, 2014 WL 6765831, at *9 (S.D.N.Y. Dec. 1, 2014) ("[T]he Second Circuit has 'not required specific search protocols or minimization undertakings as basic predicates for upholding digital search warrants.'"); *United States v. D'Amico*, 734 F. Supp. 2d 321, 367 (S.D.N.Y. 2010) ("[B]ecause there was probable cause for an all-records search, many of the privacy concerns informing the Ninth Circuit's decision in *CDT* are far less prevalent here").

In addition, it is important to recognize that even the *CDT I* suggestions were a byproduct of the unique privacy concerns that are raised by searches of third-parties' sensitive information and property who are not themselves a subject or target of a criminal investigation and/or of companies that maintain highly sensitive or confidential records of other people unrelated to, and independent of, the defendant's criminal activity. *CDT I*, 539 F.3d at 993-94. By contrast, the facts of this case are so dramatically different that it would have been in the issuing magistrate's sound judgment to issue the warrant without the special protocols and requirements described in the *CDT I* opinion, even if that were the law or practice in this district, which it is not. For instance, unlike in *CDT*, the person with the reasonable expectation of privacy—the defendant—

wholly inapplicable because the search warrant was sufficiently particular under the Fourth Amendment. Indeed, the defendant's Motion does not even challenge the search warrant's particularity.

was also the subject of a criminal investigation, and the government has articulated and the magistrate judge found probable cause to believe that the digital media at issue contained evidence of his offenses. That evidence—not only contraband, but forensic evidence of a device's usage history—might have been found anywhere in the media. The search of defendant's devices "produced only evidence pertaining to" the crimes identified on the warrant application. *King*, 2010 WL 653021 at *25 (distinguishing *CDT* in part on that basis). Additionally, there is no reason to believe that the defendant maintains highly sensitive or confidential records of other people unrelated to, and independent of, defendant's criminal activity, the private nature of human trafficking notwithstanding. Further, unlike in *CDT*, this case required officers to search not just for discrete data on a hard drive, but for evidence of user attribution and context regarding the devices' use. As the search warrant's supporting affidavit explained, it is necessary in this case to show not just that particular files were on the computer, but also to show who used the computer, to what purpose, and how. *See* Estes Aff. ¶¶ 34-35. As explained above, that need further demonstrates the reasonableness of the government's retention of original and mirror copies of the storage media in this case. *See, e.g.*, *Ganias*, 824 F.3d at 216; *see, e.g.*, *Johnson*, 789 F.3d at 941-43; *Scully*, 108 F. Supp. 3d at 100-01.[8]

Accordingly, under the circumstances, it was reasonable for the Court to authorize a search warrant that included, among other things, an Attachment B that appropriately cabined the

[8] The defendant's Motion argues, without any legal support, that it was unreasonable for the government to search the electronic media identified in Attachment A of the search warrant without a "taint team to insulate the prosecutor and case agents from exposure to material that was outside the scope of the warrant." *See* Mot. 5. However, given that the defendant does not contend that the relevant electronic media contain privileged materials, it is unclear why the defendant believes it would be necessary for the government to enlist a "taint team." A search of a premises, for example, could no doubt be searched by case agents despite only some items on the premises being seizable.

government's search of the electronic devices by identifying the target (*i.e.*, the defendant) and criminal conduct under investigation, as well as specifying particular categories of information to be seized. No further minimization procedures were required under the Fourth Amendment, and this Court should adhere to the long-standing and widely accepted practice in the Second Circuit of eschewing *ex ante* judicial restrictions on the execution of the warrant.

C. The Good Faith Exception Applies

If the Court were to find that the government's retention of electronic evidence violates Rule 41 or the Fourth Amendment, then the government argues in the alternative that the extraordinary remedy of suppression would be inappropriate because the "good-faith exception" to the exclusionary rule established by *United States v. Leon*, 468 U.S. 897 (1984) applies in this case.

The purpose of the exclusionary rule is to deter police misconduct. Accordingly, "evidence obtained in objectively reasonable reliance on a subsequently invalidated search warrant" should generally not be excluded. *Id.* at 922. "[W]hen an officer acting with objective good faith has obtained a search warrant from a judge or magistrate and acted within its scope," then "excluding the evidence will not further the ends of the exclusionary rule in any appreciable way" because "[e]xcluding the evidence can in no way affect his future conduct unless it is to make him less willing to do his duty." *Id.* at 920-21. Hence, suppression of evidence is a "last resort," *Hudson v. Michigan*, 547 U.S. 586, 591 (2006), appropriate only when law enforcement conduct is "sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system." *Herring v. United States*, 129 S.Ct. 695, 702 (2009).

Here, there is no evidence to suggest that the agents intentionally or deliberately disregarded any provision of Rule 41 or the Fourth Amendment; instead agents acted objectively reasonably in relying on the search warrant. *See, e.g.*, *Alston*, 2016 WL 2609521, at *4 (citing *United States v. Pangburn*, 983 F.2d 449, 455 (2d Cir. 1993) (quotations omitted)) (explaining that suppression was not an appropriate remedy for a delay in forensic extraction); *United States v. Cardona*, No. 14–CR–314, 2015 WL 769577, at *7 (S.D.N.Y. Feb. 24, 2015) (quoting *United States v. Burke*, 517 F.2d 377, 386–87 (2d Cir. 1975)) (describing standard for suppression); *see also* Fed. R. Crim. P. 52(a) ("Any error, defect, irregularity, or variance that does not affect substantial rights must be disregarded"). The circumstances present here made it objectively reasonable for agents to execute this Rule 41 search warrant in a manner consistent with practices that have long been upheld by federal courts, including the Second Circuit. *See, e.g.*, *Galpin*, 720 F.3d at 451; *Scully*, 108 F. Supp. 3d at 100-01; *accord Ganias II*, 824 F.3d at 221-24 (refusing to suppress evidence retained for several years based on the government's objective reasonable reliance on a Rule 41 warrant to search electronic evidence). Additionally, the extraordinary remedy of suppression would serve no deterrent purpose because tTFO Estes acted pursuant to a search warrant that the government obtained after disclosing to the magistrate judge all relevant facts relating to the forensic review of the electronic devices. *See* Estes Aff. ¶¶ 34-35.

In *Leon*, the Supreme Court articulated two exceptions that would warrant suppression: (1) if the warrant was based on an affidavit "so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable" or (2) if the warrant was "so facially deficient — *i.e.*, in failing to particularize the place to be searched or the things to be seized —

that the executing officers c[ould not have] reasonably presume[d] it to be valid." 468 U.S. at 923. Here, the search warrant at issue does not fall within either category of excludable warrants -- there is no dispute that ample probable cause supported issuance of the search warrant, and the warrant was sufficiently particular to enable the executing officers to understand where they were authorized to search and what they were authorized to seize.

Therefore, even if the Court determines that the execution of the search warrant violated the Fourth Amendment, the evidence obtained should not be suppressed, as the good faith exception applies.

D. CONCLUSION

For the reasons explained above, the Court should deny the defendant's motion to suppress evidence derived from the search warrant.

Respectfully submitted, this 23rd day of February, 2018.

CHRISTINA E. NOLAN
United States Attorney

By: */s/ Abigail E. Averbach*
Abigail E. Averbach
Assistant U.S. Attorney
P.O. Box 570
Burlington, VT 05402-0570
(802) 951-6725
abigail.e.averbach@usdoj.gov

JOHN M. GORE
Acting Assistant Attorney General
Civil Rights Division

By: */s/ Jared Fishman*
JARED FISHMAN
Special Litigation Counsel

EMILY SAVNER
Trial Attorney
Civil Rights Division, Criminal Section
U.S. Department of Justice
601 D Street, NW, 5th Floor
Washington, DC 20530
Telephone: (202) 598-1877
Jared.Fishman2@usdoj.gov

Certificate of Service

By filing the above document this day via the Court's electronic filing system, I certify that a copy will be served on William Kraham and David Williams, Counsels for Defendant, via ECF.

Dated: February 23, 2018
Burlington, Vermont

By: /s/ *Abigail E. Averbach*
Abigail E. Averbach
Assistant U.S. Attorney
P.O. Box 570
Burlington, VT 05402-0570
(802) 951-6725
abigail.e.averbach@usdoj.gov